AF
JPW

IN THE

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT(S):	Hsu et al.
APP. NO.:	09/896,255
FILED:	June 28, 2001
TITLE:	System And Method For Efficiently Performing A Data Encryption Operation
EXAMINER:	Tran, E.
ART UNIT:	2134
ATTY DKT NO:	50P4299.01/1575

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, on the date printed below:

Dated: 9/29/06

Gregory J. Koerner

RESPONSE TO NOTIFICATION OF NON-COMPLIANT APPEAL BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

This Response to Notification is being submitted in response to the Notification of Non-Compliant Appeal Brief mailed on September 20, 2006.

Amended Appeal Brief

In order to respond fully to the present Notification of Non-Compliant Appeal Brief, Applicants herewith submit the attached amended Appeal Brief. In the amended Appeal Brief, Applicants have added an Evidence Appendix (9) to indicate "None," and added a Related Proceedings Appendix (10) to also indicate "None." Furthermore, Applicants have amended the Status of Claims section to indicate the status of claim 25. Applicants therefore submit that the informalities indicated on the Notification of Non-Compliant Appeal Brief have been addressed in the amended Appeal Brief.

Respectfully Submitted,

Date: 9/26/06 By: _____

Gregory J. Koerner
Registration No. 38,519
Redwood Patent Law
1291 East Hillsdale Boulevard, Suite 205
Foster City, California 94404
(650) 358-4000

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/896,255	06/28/2001	Sherry Chu-Hsin Hsu	50P4299.01/1575	9177

24272 7590 09/20/2006

EXAMINER	

Gregory J. Koerner
Redwood Patent Law
1291 East Hillsdale Boulevard
Suite 205
Foster City, CA 94404

ART UNIT	PAPER NUMBER

DATE MAILED: 09/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Notification of Non-Compliant Appeal Brief (37 CFR 41.37)	Application No. 09/896,255	Applicant(s) HSU ET AL.	
	Examiner ELLEN TRAN	Art Unit 2134	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

The Appeal Brief filed on *07 June 2006* is defective for failure to comply with one or more provisions of 37 CFR 41.37.

To avoid dismissal of the appeal, applicant must file anamended brief or other appropriate correction (see MPEP 1205.03) within **ONE MONTH or THIRTY DAYS** from the mailing date of this Notification, whichever is longer. **EXTENSIONS OF THIS TIME PERIOD MAY BE GRANTED UNDER 37 CFR 1.136.**

1. ☒ The brief does not contain the items required under 37 CFR 41.37(c), or the items are not under the proper heading or in the proper order.

2. ☒ The brief does not contain a statement of the status of all claims, (e.g., rejected, allowed, withdrawn, objected to, canceled), or does not identify the appealed claims (37 CFR 41.37(c)(1)(iii)).

3. ☐ At least one amendment has been filed subsequent to the final rejection, and the brief does not contain a statement of the status of each such amendment (37 CFR 41.37(c)(1)(iv)).

4. ☐ (a) The brief does not contain a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number and to the drawings, if any, by reference characters; and/or (b) the brief fails to: (1) identify, for each independent claim involved in the appeal and for each dependent claim argued separately, every means plus function and step plus function under 35 U.S.C. 112, sixth paragraph, and/or (2) set forth the structure, material, or acts described in the specification as corresponding to each claimed function with reference to the specification by page and line number, and to the drawings, if any, by reference characters (37 CFR 41.37(c)(1)(v)).

5. ☐ The brief does not contain a concise statement of each ground of rejection presented for review (37 CFR 41.37(c)(1)(vi))

6. ☐ The brief does not present an argument under a separate heading for each ground of rejection on appeal (37 CFR 41.37(c)(1)(vii)).

7. ☐ The brief does not contain a correct copy of the appealed claims as an appendix thereto (37 CFR 41.37(c)(1)(viii)).

8. ☒ The brief does not contain copies of the evidence submitted under 37 CFR 1.130, 1.131, or 1.132 or of any other evidence entered by the examiner **and relied upon by appellant in the appeal**, along with a statement setting forth where in the record that evidence was entered by the examiner, as an appendix thereto (37 CFR 41.37(c)(1)(ix)).

9. ☒ The brief does not contain copies of the decisions rendered by a court or the Board in the proceeding identified in the Related Appeals and Interferences section of the brief as an appendix thereto (37 CFR 41.37(c)(1)(x)).

10. ☐ Other (including any explanation in support of the above items):

1. Brief does not contain required items under 37 CFR 41.37 (c) (1) . Evidence appendix and Related procedings appendix is required.
2. Status of claims does not mentionthe status of claim 25.
8. Evidence appendix must include copies of evidence or an indication of " None".
9. Related proceedings appendix must include copies of decision by court or Board of Appeals or an indication of " None".

TRACEY YOUNG
PATENT APPEAL CENTER SPECIALIST

IN THE

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT(S):	Hsu et al.
APP. NO.:	09/896,255
FILED:	June 28, 2001
TITLE:	System And Method For Efficiently Performing A Data Encryption Operation
EXAMINER:	Tran, E.
ART UNIT:	2134
ATTY DKT NO:	50P4299.01/1575

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, on the date printed below:

Dated: 9/29/06

Gregory J. Koerner

APPEAL BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

The following Appeal Brief is submitted in an appeal from the Final Office Action of January 24, 2006 in the above-referenced Patent Application.

(1) Real parties in interest

The real parties in interest in the above-referenced patent application are Sony Corporation, a Japanese corporation with offices in Tokyo, Japan, and Sony Electronics Inc., a Delaware corporation with offices in New Jersey.

(2) Related appeals and interferences

To the present knowledge of Appellants' legal representative, there are currently no related appeals or interference proceedings in progress which will directly affect, or be directly affected by, or have a bearing on the Board's decision in the present Appeal.

(3) Status of Claims

Claims 1-3, 5-23, and 25-42 stand rejected under 35 U.S.C. § 102(e). Claims 4 and 24 stand rejected under 35 U.S.C. § 103(a). The rejections of claims 1-3, 5-23, and 25-41 and the rejections of claims 4 and 24 are being appealed.

(4) Status of Amendments

On January 24, 2006, a Final Office Action in the present Application was mailed to Applicants' Representative. In response, on April 6, 2006, the Applicants filed a Notice of Appeal in the present Application.

(5) Summary of Claimed Subject Matter

In accordance with one embodiment of the present invention, a central processing unit (CPU) 114 initially monitors an electronic system 110 until performance of a data encryption operation is required by any appropriate entity. When a data encryption operation is required in the electronic system 110, then the CPU 114 creates an encryption structure 312 that includes one or more command structures 412. The CPU 114 stores the resultant encryption structure 312 into a memory device 126 that is coupled to the electronic system 110. The CPU 114 also selectively programs one or more local control registers 716 of a DMA engine 214 to provide relevant information regarding the required data encryption operation for local access by the DMA engine 214 of the electronic system 110.

Next, the CPU 114 instructs the DMA engine 214 to assume control and perform the required data encryption operation. In certain embodiments, the CPU 114 sets a start bit in a start register 812 of the local control registers 716 to instruct the DMA engine 214 to perform the required data encryption operation. The CPU 114 then advantageously begins to perform other processing tasks for the electronic system 110.

In response, a state machine 712 of the DMA engine 214 copies a designated command structure 412 from the memory device 126 into local command registers 720 that are coupled to the DMA engine 214. The DMA engine

214 then references data encryption information in the control registers 716 and command registers 720 to efficiently control the required data encryption operation. During the data encryption operations, the DMA engine 214 provides source data 316 from the memory device 126 to an encryption module 710 for encrypting or decrypting. The DMA engine 214 then responsively stores the encrypted or decrypted data back into the memory device 126 as destination data 318 that may be subsequently provided to any appropriate destination entity that is coupled to the electronic system 110.

The DMA engine 214 also monitors the data encryption operation to determine whether a completion condition has occurred. If the DMA engine 214 determines that a completion condition has occurred with regard to the current data encryption operation, then the DMA engine 214 notifies the CPU 114 that a completion condition has occurred, and the DMA engine 214 then terminates the current data encryption operation.

Independent claim 1 recites "a processor coupled to said electronic system, said processor creating an encryption structure in a memory device." The foregoing subject matter is discussed in the Specification, for example, at page 15, lines 1-3 (FIG. 9), and page 9, line 30 through page 12, line 3 (FIGS. 4-6). Claim 1 next recites "said processor also selectively programming control registers to perform said data encryption operation." The foregoing subject matter is discussed in the Specification, for example, at page 15, lines 3-9 (FIG. 9), and page 13, line 17 through page 14, line 11 (FIG. 8).

Claim 1 further recites "a DMA engine coupled to said processor, said DMA engine accessing said encryption structure and said control registers." The foregoing subject matter is discussed in the Specification, for example, at page 15, lines 10-16 (FIG. 9). Claim 1 additionally recites "said DMA engine including an encryption module that utilizes command information from said encryption structure and control information from said control registers to process source data to produce destination data during said data encryption operation." The foregoing subject matter is discussed in the Specification, for example, at page 15, lines 17-25 (FIG. 9).

Independent claim 21 recites "creating an encryption structure in a memory device by utilizing a processor." The foregoing subject matter is discussed in the Specification, for example, at page 15, lines 1-3 (FIG. 9), and page 9, line 30 through page 12, line 3 (FIGS. 4-6). Claim 21 next recites "programming control registers by said processor to perform said data encryption operation." The foregoing subject matter is discussed in the Specification, for example, at page 15, lines 3-9 (FIG. 9), and page 13, line 17 through page 14, line 11 (FIG. 8).

Claim 21 further recites "accessing said encryption structure and said control registers with a DMA engine." The foregoing subject matter is discussed in the Specification, for example, at page 15, lines 10-16 (FIG. 9). Claim 21 additionally recites "processing source data with an encryption module of said DMA engine to produce destination data, said encryption module utilizing command information from said encryption structure and control information

from said control registers to perform said data encryption operation." The foregoing subject matter is discussed in the Specification, for example, at page 15, lines 17-25 (FIG. 9).

Independent claim 41 includes four elements that are recited utilizing "means plus function" language. Independent claim 41 recites "means for creating an encryption structure in a memory device." The foregoing subject matter is discussed in the Specification, for example, at page 15, lines 1-3 (FIG. 9), and page 9, line 30 through page 12, line 3 (FIGS. 4-6). Claim 41 next recites "means for programming control registers to perform said data encryption operation." The foregoing subject matter is discussed in the Specification, for example, at page 15, lines 3-9 (FIG. 9), and page 13, line 17 through page 14, line 11 (FIG. 8).

Claim 41 further recites "means for accessing said encryption structure and said control registers to thereby control said data encryption operation." The foregoing subject matter is discussed in the Specification, for example, at page 15, lines 10-16 (FIG. 9). Claim 21 additionally recites "means for processing source data to produce destination data during said data encryption operation." The foregoing subject matter is discussed in the Specification, for example, at page 15, lines 17-25 (FIG. 9).

(6) Grounds Of Rejection To Be Reviewed Upon Appeal

I. Claims 1-3, 5-23, and 25-41 as rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,708,273 to Ober et al.

I1. Claims 4 and 24 as rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No 6,708,273 to Ober et al. in view of U.S. Patent No. 6,820,203 to Okaue et al.

(7) Argument

I. 35 U.S.C. § 102(e)

On page 5 of the Final Office Action, the Examiner rejects claims 1-3, 5-23, and 25-42 under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,708,273 to Ober et al. (hereafter Ober). The Applicants respectfully traverse the rejections of claims 1-3, 5-23, and 25-41 for at least the following reasons.

It is established that, "for a prior art reference to anticipate in terms of 35 U.S.C. §102, every element of the claimed invention must be *identically* shown in a single reference". (emphasis added) *Diversitech Corp. v. Century Steps, Inc.*, 7 USPQ2d 1315, 1317 (CAFC 1988). The Applicants submit that Ober fails to identically teach every element of the claims and therefore does not anticipate the present invention.

(A). Claims 1-3, 7, 14-23, 27, and 34-40

Regarding the Examiner's rejection of independent claims 1 and 21, Applicants submit that claims 1 and 21 recite limitations that are not taught or

suggested either by the cited reference, or by the Examiner's citations thereto. For example, Applicants maintain that Ober fails to disclose the relationship between the claimed "DMA engine" and "encryption module". Claim 1 recites *"said DMA engine including an encryption module that utilizes command information from said encryption structure and control information from said control registers for processing source data to produce destination data during said data encryption operation."* (emphasis added) Similarly, claim 21 recites *"processing source data with an encryption module of said DMA engine to produce destination data, said encryption module utilizing command information from said encryption structure and control information from said control registers to perform said data encryption operation."* (emphasis added)

Ober teaches a "cryptographic co-processor" that can be substituted for a current processor to add encryption capabilities (see column 2, lines 33-65). Ober also teaches that, "[t]he cryptographic coprocessor is effectively broken down into three major components: Input/Output (I/O) blocks 2, processor blocks 4 and security blocks 6" (column 4, lines 48-51).

In addition to the foregoing "three major components", Ober teaches that "the co-processor may further include a standard direct memory access (DMA) controller circuit 42 . . . ." (see column 4, lines 51-52). However, as explicitly shown in FIG. 1, the security blocks 6 of Ober are completely separate from the DMA-32 controller circuit 42 of the cryptographic co-processor. No encryption or decryption functionality is incorporated into the DMA controller circuit

disclosed by Ober.

Applicants therefore respectfully submit that Ober fails to teach a "*DMA engine including an encryption module,*" as claimed by Applicants. On the contrary, Ober explicitly teaches a "standard direct memory access (DMA) controller circuit" without internal encryption functionality (see column 4, line 52). As support for Applicants' claimed limitations, Applicants refer the Examiner to their FIG. 9, which shows a DMA engine architecture that is significantly different from the FIG. 1 architecture disclosed by Ober.

For at least the foregoing reasons, Applicants submit that claims 1 and 21 are not anticipated by the teachings of Ober. Because a rejection under 35 U.S.C. §102 requires that every claimed limitation be *identically* taught by a cited reference, and because the Examiner fails to cite Ober to identically teach the claimed invention, Applicants respectfully request reconsideration and allowance of claims 1 and 21.

Regarding the Examiner's rejection of dependent claims 2-3, 7, 14-20, 22-23, 27, and 34-40, for at least the reasons that these claims are directly or indirectly dependent from respective independent claims whose limitations are not identically taught or suggested, the limitations of these dependent claims, when viewed through or in combination with the limitations of the respective independent claims, are also not identically taught or suggested. Applicants therefore respectfully request reconsideration and allowance of dependent claims 2-3, 7, 14-20, 22-23, 27, and 34-40.

(B). Claims 5-6 and 25-26

With regard to the rejections of claims 5-6 and 25-26, the Examiner cites column 11, lines 1-43 of Ober against various functionalities of Applicants' claimed "bridge device". Applicants submit that Ober nowhere discloses a "bridge device" that performs the multiple specified functions that are recited in claims 5-6 and 25-26. In particular, Applicants submit that Ober nowhere discloses a bridge device that "facilitates bi-directional communications between said processor, one or more peripheral devices, said DMA engine, said encryption module, and said memory device" as recited in claims 5 and 25.

Furthermore, Applicants submit that Ober nowhere discloses a bridge device that "includes a processor interface for communicating with said processor, a memory interface for communicating with said memory device, and one or more peripheral interfaces for communicating with said one or more peripheral devices," as recited in claims 6 and 26. For at least the foregoing reasons, Applicants request reconsideration of the rejections of claims 5-6 and 25-26.

(C). Claims 8 and 28

With regard to the rejections of claims 8 and 28, on page 3 of the Office Action, the Examiner cites column 31, line 52 through column 32, line 67, of Ober against various elements of Applicants' claimed "command structure".

Applicants submit that, in contrast to Applicants claimed command structure, the DMA registers discussed by Ober have no effect upon encryption functionalities. For at least the foregoing reasons, Applicants therefore submit that Ober fails to disclose a "next command structure pointer" or a "control status command", as recited in claims 8 and 28. Applicants therefore respectfully request reconsideration of the rejections of claims 8 and 28.

(D). Claims 9 and 29

In the rejections of claims 9 and 29, the Examiner cites "tables 1 & 2, as well as claim 1" of Ober against various elements of Applicants' claimed "control status command". Applicants find no mention of the claimed elements of their "control status command" in either claim 1 or in tables 1 & 2 of Ober. Applicants therefore respectfully request that the Examiner explicitly associate the claimed elements of claims 9 and 29 to specific teaching in Ober so that Applicants may respond appropriately, or alternatively, to withdraw the rejections of claims 9 and 29 under 35 U.S.C. 102.

(E). Claims 10 and 30

With regard to the rejections of claims 10 and 30, the Examiner cites column 5, line 41 through column 6, line 33 of Ober against Applicants' claimed "series of command structures that are linked together in a linked list to thereby perform a series of data encryption operations." On page 4 of the

Final Office Action, the Examiner further states that Ober teaches encryption operations that are "performed at the same time or parallel execution which is interpreted to have the same meaning as 'linked list'."

In the "Free On-Line Dictionary Of Computing" (FOLDOC), a linked list is defined as "[a] data structure in which each element contains a pointer to the next element, thus forming a linear list" (emphasis added). In the context of Applicants' encryption routines, Applicants submit that a linked list with a pointer to a "next" routine indicates that the encryption routines are intended to be executed in series, and not in parallel, as suggested by the Examiner. For at least the foregoing reason, Applicants submit that Ober fails to disclose encryption command structures that are linked together in a linked list, as recited in claims 10 and 30.

(F). Claims 11 and 31

Regarding the rejections of claims 11 and 31, Ober teaches only a "standard direct memory access (DMA) controller circuit" without any type of internal encryption functionality (see column 4, line 52). Ober therefore fails to disclose that "*said DMA engine includes a state machine for controlling said data encryption operation, one or more command registers for locally storing one or more command structures from said encryption structure, said control registers, a data buffer, an encryption key register, and said encryption module,*" as recited by Applicants in claims 11 and 31. Applicants therefore respectfully request

reconsideration of the rejections of claims 11 and 31.

(G). Claims 12 and 32

In the rejections of claims 12 and 32, the Examiner cites "tables 1 & 2, as well as claim 1" of Ober against various elements of Applicants' claimed "control registers". Applicants find no mention of the claimed elements of their "control status command" in either claim 1 or in tables 1 & 2 of Ober. Applicants therefore respectfully request the Examiner to explicitly associate the claimed elements of claims 12 and 32 to specific teaching in Ober, or alternatively, to withdraw the rejections of claims 12 and 32 under 35 U.S.C. 102.

(H). Claims 13 and 33

With regard to the rejections of claims 13 and 33, on page 2 of the Office Action, the Examiner cites column 7, lines 23-24 of Ober against Applicants' claimed "processor initially creating an encryption structure in said memory device." Applicants submit that column 7, lines 23-24 of Ober is limited to discussing that the cryptographic co-processor "accesses the library and retrieves the particular encryption algorithm" (emphasis added). Applicants submit that Ober nowhere teaches a local processor device actively creating an encryption structure for use by a DMA engine, as recited in claims 13 and 33.

(I). Independent Claim 41

With regard to claim 41, "means-plus-function" language is utilized to recite elements and functionality similar to those recited in claims 1 and 21, as discussed elsewhere. Applicants therefore incorporate those remarks by reference with regard to claim 41. In addition, the Courts have frequently held that "means-plus-function" language, such as that of claim 41, should be construed in light of the Specification. More specifically, means-plus-function claim elements should be *construed to cover the corresponding structure, material or acts described in the specification,* and equivalents thereof.

In particular, independent claim 41 recites "means for creating an encryption structure in a memory device." The foregoing subject matter is discussed in the Specification, for example, at page 15, lines 1-3 (FIG. 9), and page 9, line 30 through page 12, line 3 (FIGS. 4-6). Claim 41 next recites "means for programming control registers to perform said data encryption operation." The foregoing subject matter is discussed in the Specification, for example, at page 15, lines 3-9 (FIG. 9), and page 13, line 17 through page 14, line 11 (FIG. 8).

Claim 41 further recites "means for accessing said encryption structure and said control registers to thereby control said data encryption operation." The foregoing subject matter is discussed in the Specification, for example, at page 15, lines 10-16 (FIG. 9). Claim 21 additionally recites "means for processing source data to produce destination data during said data encryption operation." The foregoing subject matter is discussed in the Specification, for example, at page 15,

lines 17-25 (FIG. 9).

Applicants respectfully submit that, in light of the substantial differences between the teachings of Ober and Applicants' invention as disclosed in the Specification, claim 41 is therefore not anticipated or made obvious by the teachings of Ober. Because a rejection under 35 U.S.C. §102 requires that every claimed limitation be *identically* taught by a cited reference, and because the Examiner fails to cite Ober to identically teach the claimed invention, Applicants respectfully request reconsideration and allowance of claim 41.

II. 35 U.S.C. § 103

In paragraph 6 of the Office Action, the Examiner rejects claims 4 and 24 under 35 U.S.C. § 103 as being unpatentable over Ober in view of U.S. Patent No. 6,820,203 to Okaue et al. (hereafter Okaue). The Applicants respectfully traverse these rejections for at least the following reasons.

Applicants maintain that the Examiner has failed to make a *prima facie* case of obviousness under 35 U.S.C. § 103(a) which requires that three basic criteria be met, as set forth in M.P.E.P. §2142:

> "First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references

when combined) must teach or suggest all the claim limitations." The initial burden is therefore on the Examiner to establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a).

Applicants respectfully traverse the Examiner's assertion that modification of the device of Ober according to the teachings of Okaue would produce the claimed invention. Applicants submit that Ober in combination with Okaue fail to teach a substantial number of the claimed elements of the present invention. Furthermore, Applicants also submit that neither Ober nor Okaue contain teachings for combining the cited references to produce the Applicants' claimed invention. The Applicants therefore respectfully submit that the obviousness rejections under 35 U.S.C §103 are improper.

Regarding the Examiner's rejection of dependent claims 4 and 24, for at least the reasons that these claims are indirectly dependent from respective independent claims whose limitations are not identically taught or suggested, the limitations of these dependent claims, when viewed through or in combination with the limitations of the respective independent claims, are also not identically taught or suggested. Applicants therefore respectfully request reconsideration and allowance of dependent claims 4 and 24 so that these claims may issue in a timely manner.

Furthermore, the Court of Appeals for the Federal Circuit has held that "obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching, suggestion, or

incentive supporting the combination." In re Geiger, 815 F.2d 686, 688, 2 U.S.P.Q.2d 1276, 1278 (Fed. Cir. 1987). Applicants submit that the cited references do not suggest a combination that would result in Applicants' invention, and therefore the obviousness rejection under 35 U.S.C §103 is improper.

For at least the foregoing reasons, the Applicants submit that claims 4 and 24 are not unpatentable under 35 U.S.C. § 103 over Ober in view of Okaue, and that the rejections under 35 U.S.C. § 103 are thus improper. The Applicants therefore respectfully request reconsideration and withdrawal of the rejections of claims 4 and 24 under 35 U.S.C. § 103.

SUMMARY

For all the foregoing reasons, it is earnestly and respectfully requested that the Board of Patent Appeals and Interferences reverse the rejections of claims 1-41, so that the present Application may be allowed and pass to issue in a timely manner.

Respectfully Submitted,

Hsu et al.

Date: 9/26/06 By: _____

Gregory J. Koerner, Esq.
Registration No. 38,519
Redwood Patent Law
1291 East Hillsdale Boulevard, Suite 205
Foster City, California 94404
(650) 358-4000

(8) Claims Appendix

1. An apparatus for performing a data encryption operation in an electronic system, comprising:

a processor coupled to said electronic system, said processor creating an encryption structure in a memory device, said processor also selectively programming control registers to perform said data encryption operation;

a DMA engine coupled to said processor, said DMA engine accessing said encryption structure and said control registers, said DMA engine including an encryption module that utilizes command information from said encryption structure and control information from said control registers to process source data to produce destination data during said data encryption operation.

2. The apparatus of claim 1 wherein said data encryption operation includes at least one of a data encryption process and a data decryption process.

3. The apparatus of claim 2 wherein said memory device receives said source data from a source entity coupled to said electronic system, said memory device responsively storing said source data into a source data memory location until said encryption module requires said source data to perform said data encryption operation.

4. The apparatus of claim 2 wherein said electronic system is implemented as one of an audio/visual electronic device, a consumer electronics device, a portable electronics device, and a computer device.

5. The apparatus of claim 2 wherein said electronic system includes a bridge device that facilitates bi-directional communications between said processor, one or more peripheral devices, said DMA engine, said encryption module, and said memory device.

6. The apparatus of claim 5 wherein said bridge device includes a processor interface for communicating with said processor, a memory interface for communicating with said memory device, and one or more peripheral interfaces for communicating with said one or more peripheral devices.

7. The apparatus of claim 2 wherein said encryption structure includes at least one command structure that has command information for performing said data encryption operation.

8. The apparatus of claim 7 wherein said command structure includes a starting source address, a starting destination address, a transfer-bytes total field, a next command-structure pointer, and a control status command.

9. The apparatus of claim 8 wherein said control status command includes an encryption/decryption field to indicate whether to perform one of said encryption process and said decryption process, an enabled/disabled field to indicate whether said data encryption operation is currently enabled, an interrupt field to designate whether an interrupt should occur following said data encryption operation, a last command field to indicate a final command structure in a linked list, and a transfer path identifier to indicate a source entity for said source data and a destination entity for destination data.

10. The apparatus of claim 2 wherein said encryption structure includes a series of command structures that are linked together in a linked list to thereby perform a series of data encryption operations.

11. The apparatus of claim 2 wherein said DMA engine includes a state machine for controlling said data encryption operation, one or more command registers for locally storing one or more command structures from said encryption structure, said control registers, a data buffer, an encryption key register, and said encryption module.

12. The apparatus of claim 2 wherein said control registers include a start register that said processor may program to start said data encryption operation, a halt/resume register that said processor may program to halt or resume said data encryption operation, a clear interrupt register that said processor may program to clear an interrupt of said data encryption operation, a link list address register that said processor may program with a physical address in said memory device of a first command structure in said encryption structure, and a status register that said DMA engine may program to indicate a current status of said data encryption operation.

13. The apparatus of claim 2 wherein said processor initially creates said encryption structure in said memory device, said encryption structure including one or more command structures that each include command information for performing a separate data encryption operation.

14. The apparatus of claim 13 wherein said processor programs said control registers with data encryption information that is then locally available to said DMA engine for performing said data encryption operation.

15. The apparatus of claim 14 wherein said processor instructs said DMA engine to perform said data encryption operation after programming said control registers, said processor then releasing control of said data encryption operation and performing other system processing tasks for said electronic system.

16. The apparatus of claim 15 wherein said DMA engine copies one or more designated command structures from said encryption structure in said memory device into one or more command registers that are locally coupled to said DMA engine.

17. The apparatus of claim 16 wherein said DMA engine controls said data encryption operation by referring to said control registers and said command registers.

18. The apparatus of claim 17 wherein a state machine coupled to said DMA engine transfers said source data from said memory device to a data buffer coupled to said encryption module, said encryption module responsively performing at least one of said data encryption process and said data decryption process to produce said destination data, said state machine then storing said destination data back into said memory device.

19. The apparatus of claim 18 wherein said DMA engine detects a completion condition while performing said data encryption operation, said DMA engine responsively notifying said processor regarding said completion condition.

20. The apparatus of claim 19 wherein said processor transfers said destination data from said memory device to a destination entity that is coupled to said electronic system.

21. A method for performing a data encryption operation in an electronic system, comprising:

creating an encryption structure in a memory device by utilizing a processor;

programming control registers by said processor to perform said data encryption operation;

accessing said encryption structure and said control registers with a DMA engine; and

processing source data with an encryption module of said DMA engine to produce destination data, said encryption module utilizing command information from said encryption structure and control information from said control registers to perform said data encryption operation.

22. The method of claim 21 wherein said data encryption operation includes at least one of a data encryption process and a data decryption process.

23. The method of claim 22 wherein said memory device receives said source data from a source entity coupled to said electronic system, said memory device responsively storing said source data into a source data memory location until said encryption module requires said source data to perform said data encryption operation.

24. The method of claim 22 wherein said electronic system is implemented as one of an audio/visual electronic device, a consumer electronics device, a portable electronics device, and a computer device.

25. The method of claim 22 wherein said electronic system includes a bridge device that facilitates bi-directional communications between said processor, one or more peripheral devices, said DMA engine, said encryption module, and said memory device.

26. The method of claim 25 wherein said bridge device includes a processor interface for communicating with said processor, a memory interface for communicating with said memory device, and one or more peripheral interfaces for communicating with said one or more peripheral devices.

27. The method of claim 22 wherein said encryption structure includes at least one command structure that has command information for performing said data encryption operation.

28. The method of claim 27 wherein said command structure includes a starting source address, a starting destination address, a transfer-bytes total field, a next command-structure pointer, and a control status command.

29. The method of claim 28 wherein said control status command includes an encryption/decryption field to indicate whether to perform one of said encryption process and said decryption process, an enabled/disabled field to indicate whether said data encryption operation is currently enabled, an interrupt field to designate whether an interrupt should occur following said data encryption operation, a last command field to indicate a final command structure in a linked list, and a transfer path identifier to indicate a source entity for said source data and a destination entity for destination data.

30. The method of claim 22 wherein said encryption structure includes a series of command structures that are linked together in a linked list to thereby perform a series of data encryption operations.

31. The method of claim 22 wherein said DMA engine includes a state machine for controlling said data encryption operation, one or more command registers for locally storing one or more command structures from said encryption structure, said control registers, a data buffer, an encryption key register, and said encryption module.

32. The method of claim 22 wherein said control registers include a start register that said processor may program to start said data encryption operation, a halt/resume register that said processor may program to halt or resume said data encryption operation, a clear interrupt register that said processor may program to clear an interrupt of said data encryption operation, a link list address register that said processor may program with a physical address in said memory device of a first command structure in said encryption structure, and a status register that said DMA engine may program to indicate a current status of said data encryption operation.

33. The method of claim 22 wherein said processor initially creates said encryption structure in said memory device, said encryption structure including one or more command structures that each include command information for performing a separate data encryption operation.

34. The method of claim 33 wherein said processor programs said control registers with data encryption information that is then locally available to said DMA engine for performing said data encryption operation.

35. The method of claim 34 wherein said processor instructs said DMA engine to perform said data encryption operation after programming said control registers, said processor then releasing control of said data encryption operation and performing other system processing tasks for said electronic system.

36. The method of claim 35 wherein said DMA engine copies one or more designated command structures from said encryption structure in said memory device into one or more command registers that are locally coupled to said DMA engine.

37. The method of claim 36 wherein said DMA engine controls said data encryption operation by referring to said control registers and said command registers.

38. The method of claim 37 wherein a state machine coupled to said DMA engine transfers said source data from said memory device to a data buffer coupled to said encryption module, said encryption module responsively performing at least one of said data encryption process and said data decryption process to produce said destination data, said state machine then storing said destination data back into said memory device.

39. The method of claim 38 wherein said DMA engine detects a completion condition while performing said data encryption operation, said DMA engine responsively notifying said processor regarding said completion condition.

40. The method of claim 39 wherein said processor transfers said destination data from said memory device to a destination entity that is coupled to said electronic system.

41. An apparatus for performing a data encryption operation in an electronic system, comprising:

means for creating an encryption structure in a memory device;

means for programming control registers to thereby facilitate efficiently performing said data encryption operation;

means for accessing said encryption structure and said control registers to thereby control said data encryption operation; and

means for processing source data to produce destination data during said data encryption operation.

42. An apparatus for performing a data processing operation in an electronic system, comprising:

a processor coupled to said electronic system for creating a data structure in a memory device, said processor also selectively programming control registers to thereby facilitate efficiently performing said data processing operation;

an engine coupled to said processor for accessing said data structure and said control registers to thereby control said data processing operation; and

a processing module coupled to said engine for processing source data to produce destination data during said data processing operation.

(9) Evidence Appendix: None.

(10) Related Procedings Appendix: None.